(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification[7]: G07F 7/00

(21) International Application Number: PCT/IB01/01462

(22) International Filing Date: 15 August 2001 (15.08.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/659,781   11 September 2000 (11.09.2000)   US

(71) Applicant: NOKIA CORPORATION [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(71) Applicant (for LC only): NOKIA INC. [US/US]; 6000 Connection Drive, Irving, TX 75039 (US).

(72) Inventors: ASOKAN, Nadarajah; Ankkurinvarsi 6 K, FIN-02320 Espoo (FI). GINZBOORG, Philip; Ylakaupinkuja 1 B 10, FIN-02360 Espoo (FI).

(74) Agents: BRUNDIDGE, Carl, I. et al.; Antonelli, Terry, Stout & Kraus, LLP, Suite 1800, 1300 North Seventeenth Street, Arlington, VA 22209 (US).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD OF BOOTSTRAPPING A TEMPORARY PUBLIC -KEY INFRASTRUCTURE FROM A CELLULAR TELECOMMUNICATION AUTHENTICATION AND BILLING INFRASTRUCTURE

(57) Abstract: A system, method and computer program for ordering, paying for and delivering goods and services through the use of certificates. These certificates insure that the buyer is only billed once for the good or service purchased and only for the correct amount. This system, method and computer program employs the authentication center used to enable access to a telecommunication infrastructure to bootstrap a public-key infrastructure. This system, method and computer program will validate the identity of the mobile station being used utilizing log term keys stored in the mobile station and an authentication center. The system, method and computer program will then utilize these keys and variables to generate digital certificates and signatures which enable the purchase of goods and services using a mobile station. The gateway will then verify the authenticity of any charges made based on the digital certificates and signatures received. Thus, a user of this system, method and computer program can purchase goods and services without fear of fraud or errors. This mobile station may be a cellular phone and when used with this system, method and computer program the cellular phone may be used similarly to a credit card but with the advantage of little possibility of fraud or error.

SYSTEM AND METHOD OF BOOTSTRAPPING A TEMPORARY PUBLIC -KEY INFRASTRUCTURE FROM A CELLULAR TELECOMMUNICATION AUTHENTICATION AND BILLING INFRASTRUCTURE

TECHNICAL FIELD

The invention relates to a system and method of bootstrapping a public -key infrastructure to enable secure payment of goods and services using a mobile terminal. More particularly, the invention is a system and method in which subscribers of a cellular telecommunication system can buy goods and services from sellers and arrange for payment through the subscriber=s telephone bill using a mobile terminal which ensures that errors and fraud do not take place relating to the payment.

BACKGROUND ART

It has been common for buyers to pay for goods and services using credit and debit cards. The use of credit cards has eliminated the need to carry large amounts of cash in order to pay for these goods and services. Further, the use of a credit card has eliminated the need for car rental agencies and hotels to require large deposits in order to assure return of vehicles or to reserve rooms. Thus, the use of credit cards has facilitated the transacting of business and thus provides a significant convenience to the buyer. However, credit cards have also facilitated the occurrence of fraud and errors in which the customer is double billed for the same item or billed the incorrect amount.

With the explosion in Internet access and usage, an increasing volume of business is occurring between individuals and firms, who have never seen each other, let alone e ngaged in any prior business transactions. Currently, a typical Internet user would have a browser installed in his local computer or server such as Internet Explorer™ or Netscape™. Using this browser, the user would access an Internet service provider, such as America-On-Line (AOL™), via a modem over the local public switched telephone network (PSTN). Once logged onto the Internet server, the user may utilize one of the many search engines, such as Yahoo™ or Lycos™, to specify search terms. The us er may also use a web crawler, spider or robot to attempt to find a product, service or information desired. The search engine or web crawler would then respond with a list of web sites which matched the search terms the user provided. The user would then log onto a web site and view the products or services available for sale. If the user decides to buy the item from the web site, the firm operating the web site would again frequently request a credit card number be entered by the user in order to pay f or the product or service. Once the credit card charge is approved, the operator of the web site will then typically ship the item to the user. In the case where the item ordered is digital in format, such as software, graphics, text, video, or music, th e item

ordered maybe downloaded into the user=s PC, server, lap top, palm computer or other processor -based system.

With the advent of cellular phones with and without wireless access protocol (WAP), a user may also Asurf@ the Internet and order goods and services directly through the WAP-capable phone or a processor-based system connected to the cellular phone in a similar manner as that used with a PC. Thus, a user may order goods and services from anywhere with a cellular phone, satellite phone, or ot her type of mobile station. Therefore, a person could be sitting in the middle of a remote area, many miles away from another human being, let alone a telephone line, and order a video game from a web site on the other side of the planet and download it into his palm computer connected to a cellular or a standalone WAP or HTML (Hypertext Markup Language) capable phone and play the game on the spot.

However, the user or consumer may not know who is operating the web site and may have a legitimate fear of supplying a credit card number over the Internet to a stranger who may or may not deliver the desired product. Further, the user may be concerned that the agreed upon price will not be the price actually charged to his credit card even when the buyer is d ealing directly in a face to face transaction with the seller. In addition, there is also the possibility even in a face to face transaction that the buyer may be double billed for the same item. Also, in an Internet transaction there is no guarantee tha t the goods will be delivered if the web site operator is less than honest.

Credit card companies have attempted to resolve the issues related to double billing or billing the incorrect amount by providing dispute resolution services in which a customer ma y challenge a charged amount and the credit card company will launch an investigation. However, such an investigation may take a long time and the buyer is not guaranteed of a satisfactory resolution. In the case of fraud due to a stolen credit card, the credit card company will normally limit liability if the card is promptly reported as stolen. In the case of a debit card, the bank may not be required to limit liability in case of loss or theft.

Other methods utilized to prevent fraud and error in com mercial transactions has been through the use of digital signatures that may not be repudiated. In public key systems, an entity called the certification authority (CA) performs two central functions: issuance and revocation of certificates. A certificat e is used to connect a name or an authorization, such as permission to make purchases, to a public signature verification key. The certificate is signed by the CA. To verify the certificate an authentic copy of CA's public signature verification key is required. For example, assuming a person or entity has the public key of a certain CA (CA1). This person or entity can verify certificates issued by a certain CA (CA2), only if CA2's public key has been certified by CA1. This type of cross -certification of CAs is referred to as a "public key infrastructure" (PKI). Thus, in order for digital signatures to have widespread usage such digital signatures require the presence of a global PKI which is difficult to develop since it requires

2

contracts and agreements between a large number of parties. Attempts to create such a global PKI system have so far met with failure. Public key certificates and cross certification are discussed in further detail in Section 13.4.2 "public key certificates" and Section 13.6.2 "Trust models involving multiple certification authorities" of Handbook of Applied Cryptography by A. J. Menezes et al., CRC Press 1997, ISBN 0 - 8493-8523-7, which are incorporated herein by reference.

Therefore, what is needed are a system and method whi ch allows a user or consumer to pay for goods and services while ensuring that an hacker or criminal may not listen in or tap into a payment transaction between a legitimate buyer and seller and later use this knowledge to make purchases which are charged to the legitimate user. This system and method should further not allow the legitimate user from repudiating legitimate charges he has made. This system and method should also prevent a seller from forging payment transactions in the name of a legitimate consumer. This system and method should also not require the establishment of a new infrastructure in order to operate properly.

DISCLOSURE OF INVENTION

An embodiment of the present invention provides a method of ordering, paying for and delivering goods and services using a mobile station. This method starts by authenticating the mobile station is permitted access to a telecom infrastructure. It then accesses a gateway by the mobile station and transmits an identification code for the mobile station t o the gateway. This method then requests a digital certificate by the mobile station from the gateway used for ordering and paying for a product or service from a seller using the certificate. The method then verifies the identity of the mobile station b y the gateway accessing an authentication center and comparing variables computed by the mobile station and variables computed by the gateway. It then verifies the legitimacy of the gateway by comparing the variables computed by the gateway with the variables computed by the mobile station. The method delivers a digital certificate to the mobile station by the gateway when the identity of the mobile station and the gateway have been verified. It then requests a product or service from a seller and transm its a digital signature, accompanied by the digital certificate for the signature verification key, as payment to the seller.

Further, an embodiment of the present invention creates a system and computer program for ordering, paying for and delivering goo ds and services using a mobile station. This system and computer program uses a GSM authentication module to verify that the mobile station belongs to a user that can be billed. It also has a mobile station certificate acquisition module to request a dig ital certificate for the mobile station from a gateway and verify that the gateway is authorized to issue the digital certificate by comparing variables computed by the gateway and the mobile station. The system and method also has a gateway certificate generation module to verify that the mobile station is authorized. This module also

3

transmits an international mobile subscriber identifier received from the mobile station to an authentication center, and receives information using which it can verify the authenticity of the mobile station by means of a challenge-response protocol. Once verified, this module generates and issues a digital certificate to the mobile station.

These and other features of this device and method will become more apparent from t he following description when taken in connection with the accompanying drawings which show, for purposes of illustration only, examples in accordance with the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and a better understanding o f the present invention will become apparent from the following detailed description of exemplary embodiments and the claims when read in connection with the accompanying drawings, all forming a part of the disclosure of this invention. While the foregoin g and following written and illustrated disclosure focuses on disclosing example embodiments of the invention, it should be understood that the same is by way of illustration and example only and the invention is not limited thereto. The spirit and scope of the present invention are limited only by the terms of the appended claims.

The following represents brief descriptions of the drawings, wherein:

FIG. 1 is an example of an overall system diagram of an embodiment of the present invention;

FIG. 2 is a diagram of the messages passed between a mobile station, a gateway, and a home location register (HLR) that contains or is connected to an authentication center (AUC) so that the buyer maybe authenticated and ultimately receive a certificate which may be us ed to purchase goods and services;

FIG. 3 is a flowchart of the mobile stations certificate acquisition module shown in FIG. 12 as utilized in an embodiment of the present invention;

FIG. 4 is diagram showing a Global Standard for a Mobile (GSM) communicat ions authentication algorithm used in the example embodiments of the present invention;

FIG. 5 is a flowchart of the gateway certificate generation module shown in FIG. 12 as utilized in an embodiment of the present invention;

FIG. 6 is a diagram of the me ssages that pass between the mobile station and the seller in order to facilitate the purchase and payment of goods and services as utilized in an example embodiment of the present invention;

FIG. 7 is a flowchart of a buyer purchase module shown in FIG. 1 2 as utilized by an embodiment of the present invention;

4

FIG. 8 is a flowchart of the seller sales module, shown in FIG. 12, as utilized by an embodiment of the present invention;

FIG. 9 is a diagram of the messages passed between the seller and the gatewa y in order to facilitate payment to the seller for services and goods provided the buyer in an example embodiment of the present invention;

FIG. 10 is a flowchart of the seller billing module, shown in FIG. 12, as utilized in an example embodiment of the present invention;

FIG. 11 is a flowchart of the gateway billing module, shown in FIG. 12, as utilized in an example embodiment of the present invention; and

FIG. 12 is a modular configuration diagram of the embodiments of the present invention shown in FIGs. 3-5, 7, 8, 10, and 11.

BEST MODE FOR CARRYING OUT THE INVENTION

Before beginning a detailed description of the invention, mention of the following is in order. When appropriate, like reference numerals and characters maybe used to designate identical , corresponding or similar components in differing figure drawings. Further, in the detailed description to follow, exemplary sizes/models/values/ranges may be given, although the present invention is not limited to the same.

FIG. 1 illustrates an example of an overall system diagram of an embodiment of the present invention. In this example embodiment a mobile station (MS) 20 acts as an interface for the user, buyer or consumer 10 for access to the present invention. This mobile station (MS) 20 may be a WAP-capable cellular telephone, a Hypertext Markup Language (HTML) capable cellular telephone, or a cellular telephone with a processor-based system connected to it. This processor-based system may be, but not limited to, a laptop computer, palm comput er, or other portable computing devices including the WAP - capable telephone alone. The mobile station (MS) 20 communicates through the telecom infrastructure 30 to a local network operator service 70 through a gateway 60. Telecom infrastructure 30 may be , but not limited to a cellular telephone control protocol, such as GSM (Global System for Mobile Communications) telephony system, and internet protocol (IP) over wireless local area network (LAN) or any other suitable access protocol. The interface betw een the mobile station 10 and the seller 50 is to communications infrastructure 35 which may be, but not limited to, a direct physical connection, correct short range radio frequency (RF) connection, an IP connection, or any other suitable means of communi cation. In turn the seller 50 may communicate to the gateway 60 and thus the local network operator service 70 through, but not limited to, an internet protocol packet-switched network, a dial-up line over the public switched telephone network, or any oth er suitable means of communications. Therefore, the embodiments of the present invention are not limited to communications using the Internet. Further, the local network operator service 70 may communicate to the buyer=s 10 home network operator service 80 directly through the PSTN or via the Internet. In addition, the home network operator service 80, the local network operator service 70 and a gateway 60 are all considered part of the mobile telephone infrastructure for billing and authentication 90 which serves to facilitate the purchase of goods and services.

In FIG. 1 it should be noted that the assumption is made that user 10 is not within the home network operator service 80 area. However, the embodiments of the present invention will operate when the user 10 is in the home network operator service 80 area and thus the home network operator service 80 and the local network operator service 70 may be one and the same entity.

When the user or consumer 10 is not in his home network operator service 8 0 area, the user 10 may still make purchases from seller 50 if a roaming agreement exists between the local network operator

service 70 and the home network operator service 80. Further, the seller 50 may be anyone selling a good or service from a street flower vendor to a department or clothing store. The seller 50 may also be a seller of software or other digital products and may have a store front or may have a web site on the Internet 40. The only restriction on the seller 50 is that he be permitted by the local network operator service 70 to accept digital payment certificates from a buyer 10 and submit them to the local network operator service 70 for payment. If the user or buyer 10 is outside of his home network operator service 80 area, the loca 1 network operator service 70 will submit an accounting record of the transaction between buyer 10 and seller 50 to the user=s 10 home network operator service 80 for billing on the user=s 10 telephone bill.

Still referring to FIG. 1, using the present in vention it is possible for a buyer 10 to utilize mobile station 20 similarly to a credit card to pay for goods and services wherever the user=s home network operator service 80 has established a roaming agreement with the local network operator service 70. As with the major credit cards, this could someday be worldwide if a universal cellular phone standard is established. As will be discussed ahead, the use of the present invention eliminates the possibility of double billing a buyer 10 for a product or service or submitting an incorrect price .for payment for a particular good or service. Further, since digital signatures cannot be forged by any party that do not have access to the signing key, and since the signing key is never released outside the mobi le station 20, it would be impossible for a third party eavesdropper, hacker, criminal, or the seller to either undetectably modify payment messages generated by a legitimate payer, or generate bogus payment messages purportedly coming from a legitimate payer. In addition, the buyer or user 10 may utilize mobile station 20 wherever his home network operator service 80 has established a roaming agreement and his mobile station 20 can interface to the local network operator service 70.

A discussion will now be supplied involving the logic employed in the embodiments of the present invention. Specifically, a discussion will be provided of the flowcharts and diagrams illustrated in FIGs. 2 through 11 and the modular configuration diagram provided in FIG. 12. The flowcharts and diagrams shown in FIGs. 2 through 12, as well as the modular configuration diagram shown in FIG. 12 contain operations that correspond, for example, to code, sections of code, instructions, firmware, hardware, commands or the like, of a computer program that is embodied, for example, on a storage medium such as floppy disk, CD Rom, EP Rom, hard disk, etc. Further, the computer program can be written in any language such as, but not limited to, for example C++.

Embodiments of the presen t invention use the GSM (Global System for Mobile Communications) telephony system that employs algorithms in the mobile station (MS) 20, such as, but not limited to, cellular phones and WAP-capable cellular phones, and the a mobile telephone infrastructur e for billing and authentication 90 which controls authentication of the user 10 and mobile station 20 to prevent

7

unauthorized access to the network and to provide encryption of the transmissions between users. The GSM System is described in depth in the publication, "The GSM System for Mobile Communications" by Mouly and Pautet, Copyright 1992, which publication is incorporated herein by reference in its entirety. Security features of the GSM system are described in pages 477 through 498 of the Mouly and Pautet text. Further detail of the GSM system security is provided in ETSI publication TS 100 929 V.6.1.0 (1999) entitled ADigital cellular telecommunications system (Phase 2+); Security related network functions@ (GSM 03.20 version 6.1.0 Release 1997), which is incorporated herein by reference in its entirety. The usage of the GSM system in the present invention will be discussed in further detail in relation to the FIGs. 2-12 and in particular to FIG. 4. However, it should be noted that any other GSM like system may be used that authenticates a mobile station 20 for access to a telecom infrastructure 30. ·

FIG. 2 is a diagram of the messages passed between a mobile station 20, a gateway 60, and a home location register (HLR) authentication center (AUC) located in the home network operator service 80. In the following discussion, curly brackets { } indicate a set of one or more items, and square brackets [ ] indicate an optional item. The messages 210 through 260 enable mobile station 20, and thus a buy er 10, to receive a digital certificate which enables the buyer 10 to purchase and pay for goods and services from seller 50. A total of four messages are exchanged between mobile station 20 and gateway 60, while two messages are exchanged between gateway 60 and HLR/AUC 100. These messages will be discussed in further detail in reference to FIGs. 3 and 5. However, to summarize, message 210 is transmitted from mobile station 20 to gateway 60 and contains a session identification (SID) and an internationa l mobile subscriber identifier (IMSI). The IMSI is a unique identification number supplied for each mobile station 20 by the home network operator service 80 upon initial signing of a contract for service. The SID is a number assigned by the mobile station 20 and used to identify this particular session. The gateway 60 in turn stores the SID and IMSI in its local memory and transmits the IMSI in message 220 to the HLR/AUC 100 contained within home network operator service 80. The gateway 60 is able to i dentify which HLR /AUC 100 it needs to transmit the IMSI to based on information contained within the IMSI. As will be discussed in further detail in reference to FIG. 4, the HLR/AUC 100 responds with message 230 containing a random number (RAND) 410, a s igned response (SRES) 450, and an encryption key (Kc) 400. The gateway 60 takes the Kc 400 and uses it to compute an integrity key (K) based on the formula K = $f(\{Kc\})$, where f is a cryptographic one -way hash function known both to the gateway 60 and to t he mobile station 20. The gateway 60 would then store the SID, IMSI, RAND 440, SRES 450 and K in a single record in the gateway=s 60 memory. Thereafter, message 240 is sent from the gateway 60 to the mobile station 20 and contains RAND 440 and M1. M1 is computed based upon a message authentication code (MAC) function using integrity key (K) And RAND 440. The formula used is represented as M1 =

MAC (K, {RAND}). The purpose of a MAC is to facilitate, without the use of any additional mechanisms, assurances regarding both the source of a message and its integrity MACs have two functionally distinct parameters, a message input ({RAND}) and a secret key (K). MAC functions are discussed in further detail in sections 9.5 Akeyed hash functions (MAC=s)@ and 9.6 .3 AData Integrity Using MAC Alone@ of Handbook of Applied Cryptography by A. J. Menezes et al., CRC Press 1997, ISBN 0-8493-8523-7, which are incorporated herein by reference. Upon receipt of the RAND 440 and M1 variables, the mobile station 20 computes SRES 450 and Kc 400 based on RAND 440 and secret key (Ki) 410. Ki 410 is a secret key installed by the home network operator service 80 in the mobile station 20 upon signing up for a service plan. The mobile station 20 also computes the integrity key (K) using the formula $K = f(\{Kc\})$. The computation of Kc 400 is discussed in further detail in reference to FIG. 4.

Still referring to FIG. 2, mobile station 20 responds to the receipt of message 240 by the generating message 250 and transmitting message 250 to gateway 60. Message 250 includes SRES 450, a public key (PK), any restrictions, an alias, and M2. The public key (PK), provided by mobile station 20, is used to generate digital signatures for user 10 which act as approvals for charges made in the p urchase of goods and services. Both the restrictions and alias are optional items. Restrictions refer to limitations on transactions that may be placed. For example, user or buyer 10 may be protected from a loss or theft of mobile station 20 by limiting the amount of any given purchase, the number purchases that can be made within a particular time frame, or the time period within which the public key is valid. The alias is an alternate identification for the mobile station 20. M2 is computed based upo n another MAC function utilizing the variables K, SRES 450, PK, restrictions, and the alias. The specific formula for computation of M2 is M2 = MAC (K, {SRES}, PK, [{restrictions}], [alias]). Upon receipt of message 250, the gateway 60 generates a digital certificate (C) and stores in a record in memory the SID, IMSI, f(RAND, SRES, K), PK, restrictions, alias, and digital certificate (C). Thereafter, the gateway 60 computes M3 which is based on formula M3 = MAC (K, C). Then in message 260, the gateway 60 transmits the message 260 containing the digital certificate (C) and M3 to the mobile station 20. The digital certificate (C) may then be used to purchase goods and services from seller 50.

In an alternate embodiment of the messages shown in FIG. 2, i t is possible to enhance security of the present invention by encrypting the IMSI in message 210 using a public key supplied by the gateway 60 or some other server. In this manner it is less likely that the IMSI would be intercepted by a third party.

In a still further alternate embodiment of the messages shown in FIG. 2, it is possible to have the SID jointly selected by the mobile station 20 and the gateway 60. In this manner, tracking of the certificate in message 260 and associating it to the SID may be simplified for the gateway 60.

In another alternate embodiment of the messages shown in FIG. 2, it is possible to drop the SRES 450 in message 250 since it is already required to generate a correct M2.

In another embodiment of the messages shown in FIG. 2, it is possible for the HLR to compute the integrity key K and send it as part of message 230 to the gateway. In this case, as an alternative embodiment, instead of the integrity key (K) computed as a function of the set of encryption key (Kc) 400, it may be computed directly from the secret key (Ki) 410 and the random number (RAND) 440.

In another embodiment of the messages shown in FIG. 2, the public key (PK) may be a long term public key stored in the authentication center (AUC). In this case, PK i s included in message 230, and need not be included in message 250.

In still another embodiment of the messages shown in FIG. 2, the public key (PK) of the local network operator service 70 (denoted as PK_G) can be included in message 260. This allows the mobile station 20 to verify certificates that were issued by the operator to other entities such as sellers 50. It also allows the mobile station 20 to verify certificates that were issued to other mobile stations 20, thereby allowing the first mobile station 20 to act as a seller. Therefore, a mobile station 20 may act in one instance as a buyer and in the next instance as a seller. This would be most suitable when the product being sold is a digital product. However, any good or service may be sold t his way.

A discussion will now be provided for FIGs. 3 through 5 detailing the exchange of messages as shown in FIG. 2. FIG. 3 is a flowchart of the mobile station certificate acquisition module 1500 shown in FIG. 12. The mobile station certificate acqu isition module 1500 is used to generate messages 210 and 250 shown in FIG. 2. The mobile station certificate acquisition module 1500 also receives and processes messages 240 and 260 from a gateway 60, as shown in FIG. 2. The mobile certificate acquisiti on module 1500 includes operations 300 through 430 shown in FIG. 3.

Referring to FIG. 3, the mobile station certificate acquisition module 1500 begins execution in operation 300 and immediately proceeds to operation 310. In operation 310, a SID is genera ted which is a unique number identifying a session. In addition, the IMSI representing the international mobile subscriber identifier is retrieved and along with the SID is transmitted to gateway 60 in message 210. Thereafter, in operation 320, the mobil e station 20 will wait for receipt of message 240 from gateway 60. Upon arrival of message 240, processing will then proceed to operation 330. As previously discussed, message 240 contains a random number (RAND), and M1. M1 was computed by the gateway 6 0 utilizing a integrity key (K) and a random number (RAND) received from the HLR/AUC 100. In operation 330, mobile station 20 computes M1'. M1' is computed in the same manner by the mobile station 20 as M1 was computed by gateway 60 with the exception that encryption key (Kc) 400 is contained within the mobile station 20 itself and is used to compute integrity key (K). Utilizing the same formula used by the gateway

●   ●

60, the mobile station 20 is able to compute M1'. The formula utilized is M1' = MAC (K, { RAND}). Therefore, in operation 340 a comparison is made between M1 received from gateway 60 and M1' computed by the mobile station 20. This comparison is done in order to assure the mobile station 20, and thus user 10, that the source of message 240 is a legitimate portion of the GSM system. If M1 is not found to equal M1' in operation 340, then processing proceeds to operation 350 where execution of the mobile station certificate acquisition module 1500 is aborted and processing terminates. If operation 350 is executed the assumption is that message 240 has been corrupted or that a gateway 60 is being impersonated by an unauthorized individual.

Still referring to FIG. 3, if M1 = M1', then processing proceeds from operation 340 to operation 360. In operation 360, M2 is computed. As previously discussed, M2 is computed based upon a MAC function utilizing the variables K, SRES 450, PK, restrictions, and the alias. The specific formula for computation of M2 is M2 = MAC (K, {SRES}, PK, [{restrictions}], [alias]). Thereafter, message 250 is generated containing SRES, PK, restrictions, alias, and M2 and is transmitted to gateway 60. In operation 380 the mobile station 20 waits for receipt of message 260 from gateway 60. Upon receipt of message 260 from gateway 60 processing then proceeds to operation 390. In operation 390, M3' is computed as previously discussed above in reference to FIG. 2. M3' is computed in the same manner as M3 was computed by the gateway 60 based on formula M3 = MAC (K, C) with the exception that encryption key (Kc) 400 is contained within the mobile station 20 itself and is used to compute integrity key (K). Thereafter, processing proceeds to operation 400 where M3' is compared against M3 received in message 260 from gateway 60. If it is determined in operation 400 that M3' does not match M3, then processing proceeds to operation 410. In operation 410, processing of the mobile station certificate acquisition module 1500 is terminated. When M3' does not match M3, it is assumed that message 260 has been corrupted or that an unauthorized individual is impersonating a gateway 60. However, if M3' does match M3 in operation 400, then processing proceeds to operation 420. In operation 420, the certificate received in message 260 is stored in the memory of mobile station 20. This certificate may be used, within any associated restrictions, for the purchasing of goods and services from seller 50. Thereafter, processing for the mobile station certificate acquisition module 1500 terminates in operation 430.

FIG. 4 further details authentication in a GSM network performed by the generation of a signed response (SRES) 450 by both the mobile station (MS) 20 and the home network operator service 80 and gateway 60 which is a function of a unique secret key (Ki) 410 of the mobile station 10 and a random number (RAND) 450 as used in the logic shown in FIGs. 3 and 5. The signed response (SRES) 450 is calculated in a subscriber identification module (SIM) (not shown) located in the mobile station (MS) 20, based on Ki 410 inside the SIM and RAND 440 obtained from the network authentication center (AUC)

11

(not shown) in the home network operator service 80. Additionally, the mobile station (MS) 20 and the authentication center in the home network operator service 80 each generate a ciphering key (Kc) 400 which is a function of the same random number RAND 440 and the secret key (Ki) 410 of the mobile station 20. This authentication process is a two stage process which employs two algorithms. The first algorithm, which calculates SRES 450, is known as the A3 algorithm module 420 and the second, key generation, algorithm which computes Kc 400, which is computed each time a mobile station 20 is authenticated, is known as the A8 algorithm module 430. However, each of the operations of authentication and computing of the ciphering key (Kc) 400 requires the mobile station (MS) 20 to be programmed to perform the aforementioned computations.

Still referring to FIG. 4, the mobile switching center (not shown) located in the local network operator service 70 authenticates the mobile station 20 whenever a new mobile station (MS) 20 registers with the mobile telephone infrastructure for billing and authentication 90 and whenever a registered mobile station (MS) 20 turns on the power. Authentication in a GSM system is based on a secret key (Ki) 310 that is shared by the home network operator service 80 and the subscriber and which is different for each subscriber. The home network operator service 30 keeps the key K i 410 in the AUC and the subscriber has Ki 410 installed within SIM card of the mobile station 20, which he receives from the home network operator service 80 when the subscription contract is made. To protect the secrecy of Ki 410, the SIM is made so that the mobile station (MS) 20 cannot directly access the value of Ki 410, and can only initiate certain computations in the SIM that use Ki 410 and then receive the results of those computations. Similarly, the elements of the mobile telephone infrastructu re for billing and authentication 90, such as home location register (HLR) cannot access subscribers' keys Ki 410 directly. These network elements may only request from the AUC a result of computations that use Ki 410 as discussed above. These computations are an A3 algorithm module 420 and an A8 algorithm module 430 and are identical in the SIM of the mobile station (MS) 20 and in the AUC in the home network operator service 80.

The foregoing mentioned GSM authentication process is a two stage process. In the first stage of GSM authentication, a local network operator service 70 element, which is typically a MSC/VLR (Mobile services Switching Center/Visitor Location Register), receives an International Mobile Subscriber Identifier (IMSI) from the mobile station (MS) 20 and requests from the AUC of the home network operator service 80 one or more triplets. These triplets are composed of RAND 440, SRES 450, and Kc 400. This process begins by the mobile station 20 sending an International Mobile Subscribe r Identifier (IMSI) to MSC/VLR in the local network operator service 70. The MSC/VLR then requests authentication triplet(s) (RAND 440, SRES 450, and Kc 400) from the AUC in the home network operator service 80.

The AUC, in the home network operator serv ice 80, computes one or more triplets (RAND 440, a SRES 450, and a Kc 400) and sends them to the MSC/VLR in the local network operator service 70.

In the second stage of GSM authentication, the MSC/VLR of the local network operator service 70 authenticates the mobile station (MS) 20 by the MSC/VLR in the local network operator service 70 sending to mobile station 20 an *authentication request (RAND)* in which the message contains a RAND 140. The MS 20 then sends to the SIM, contained within MS 20, a *run GSM algorithm (RAND) request message* which again contains RAND 440. In operation 260, MS 20 sends to the SIM a *get response message*. Thereafter, the SIM replies with a response having a SRES 450 and Kc 400. Then MS 20 stores Kc 400 in the SIM by sending to the SIM a *write (Kc)* request in which the message contains Kc 400. The MS 20 sends to MSC/VLR a Radio Interface Layer 3, Mobility Management (RIL 3 -MM) protocol *authentication response* in which the SRES 450 is contained in the message. After receiving t he message the MSC/VLR, in the local network operator service 70, compares SRES 450 that it has received from the AUC in the home network operator service 80, in stage one of GSM authentication discussed the SRES 450 received from the MS 20. If the value s of the SRES 450 are determined not to be identical then authentication fails and service is not established. However, if the values are identical then authentication succeeds and service is established for the MS 20.

FIG. 5 is a flowchart of the gatewa y certificate generation module 1600, shown in FIG. 12, as utilized in an embodiment of the present invention. The gateway certificate generation module 1600 is the counterpart of the mobile station certificate acquisition module 1500 and serves to genera te a digital certificate required by buyer 10 in order to make purchases from seller 50. The gateway certificate generation module 1600 begins execution in operation 500 and immediately proceeds with operation 510. In operation 510, the gateway 60 awaits transmission of message 210 from mobile station 20. Upon receipt of message 210 from mobile station 20, the gateway 60 stores in local memory the SID and IMSI contained in message 210 and processing proceeds to operation 520. In operation 520, the gatew ay 60 generates message 220 containing the received IMSI. Based on IMSI, the gateway 20 knows which HLR/AUC the mobile station 20 is associated with and can thereby transmit message 220 thereto. Thereafter, processing proceeds to operation 536 where the gateway 60 waits for the receipt of message 230 from the HLR/AUC 100. The HLR/AUC 100 upon receipt of message 220 will reply with one or more triplets. These triplets contain RAND 440, SRES 450, and Kc 400. The gateway 60 will then proceed to compute M1 in operation 540 as previously discussed. M1 is computed based upon a message authentication code (MAC) function using integrity key (K) And RAND 440. The formula used is represented as M1 = MAC (K, {RAND}). Integrity key (K) is computed based on Kc 40 0 received from HLR/AUC 100 using the formula K = f ({Kc}). Processing them proceeds to operation 550 where

13

message 240 is generated and transmitted to mobile station 20. As previously discussed, message 240 contains RAND 440 and M1. Thereafter, process ing proceeds to operation 560 where the gateway 60 waits for message 250 from mobile station 20. Upon receipt of message 220 processing proceeds to operation 570 where M2' is computed. M2' is computed based upon a MAC function utilizing the variables to K, SRES 450, PK, restrictions, and the alias. The specific formula for computation of M2' is M2' = MAC (K, {SRES}, PK, [{restrictions}], [alias]). Processing them proceeds to operation 580 where a comparison is made between M2, received in message 250, and M2' computed by gateway 60. If M2' and M2 do not match then processing proceeds to operation 590 where the execution of the gateway certificate generation module 1600 is aborted. However, if M2' and M2 match then processing proceeds to operation 600. In operation 600, M3 is computed by the gateway 60. The gateway 60 computes M3 based on the formula M3 = MAC (K, C). In operation 610, message 260 containing the certificate and M3 are transmitted to the mobile station 20. Thereafter, processing te rminates for the gateway certificate generation module 1600 in operation 270.

Upon termination of the mobile station certificate acquisition module 1500 along with its counterpart, gateway certificate generation module 1600, the mobile station 20 has in it s possession a certificate which buyer 10 may use to purchase goods and services from seller 50. FIGs. 6 through 8 illustrate the processing involved by the embodiment of the present invention in order for buyer 10 to make purchase from seller 50.

FIG. 6 is a diagram of the messages passed between the mobile station 20 and the seller 50 in order to facilitate the purchase and payment of goods and services as utilized in an example embodiment of the present invention. A total of two messages are sent by t he mobile station 20 to seller 50. The messages sent from mobile station 20 to seller 50 include message 610 and message 630. Seller 50 in turn respond with message 620 and message 640. Message 610 contains a certificate received from gateway 60 and a request for a particular product or service. Message 620 is an invoice transmitted from seller 50 to mobile station 20. This invoice serves to notify buyer 10 through mobile station 20 of the price of the item requested. The invoice contains a seller-specific unique transaction identifier, chosen by the seller 50, and the identity of the seller 50, as assigned by the gateway 60. Message 630 includes a digital signature which serves to authorize charging the price of the invoice against the certificate su pplied. Message 640 includes the delivery of the product to the mobile station 20. In the foregoing discussion of messages 610 through 640 it has been assumed that the product or service requested is in digital format that could be downloaded to mobile station 20. However, as previously discussed the product or service an individual buyer 10 may request may be anything including such tangible items as flowers and clothing. In the case where the

14

product is a tangible item and buyer 10 and seller 50 face each other, then the request may take the form of an oral request and the delivery may take the form of handing over the flowers or other product.

In an alternate embodiment of the message configuration shown in FIG. 6, it is possible for message 610 to contain the request only, and message 630 to contain both the signature and the certificate. In this manner the seller sales module 1800, discussed in detail ahead, verifies the certificate and signature at the same time.

In a further alternate embodiment of the message configuration shown in FIG. 6, it is possible to charge for use of a product, such as a software based game, by the time of usage and not for mere delivery of the product. One method for implementing this would be for several messages 620 t o be sent to the mobile station 20 at periodic time intervals. For example, if buyer 10 requests a game and it is downloaded, an initial invoice would be sent, after which a new invoice will be sent every five minutes.

FIG. 7 is a flowchart of a buyer pur chase module 1700 shown in FIG. 12 as utilized by an embodiment of the present invention. The buyer purchase module 1700 includes operations 700 through 770 shown in FIG. 7. When a buyer 10 initiates a purchase of an item from seller 50, the buyer purcha se module 1700 begins execution in operations 700 and immediately proceeds to operation 710. In operation 710 the mobile station 20 transmits message 610 to seller 50. The mode of transmission may be any form of digital communications. Thus, if the sell er 50 is a web site, then mobile station 20 would access seller 50 through the cellular access network, via a gateway (such as a WAP gateway), and then through the Internet. However, if a face-to-face transaction is occurring between buyer 10 and seller 5 0 then communications between mobile station 20 and seller 50 may include any short range form of communications including cable, infrared, low-power radio frequency, or any other suitable means.

Still referring to FIG. 7, in operation 720 mobile station 20 will wait for receipt of message 620 from seller 50. Upon receipt of message 620 processing then proceeds to operation 730. In operation 730 the buyer 10 checks the invoice price to determine if it is valid. In operation 740, a determination is made whether invoice (I) is correct. If invoice (I) is not correct processing proceeds to operation 750 where processing of the buyer purchase module 1700 is terminated. However, if the invoice (I) is correct then processing proceeds to operation 750. In operation 750, the buyer 10 digitally signs the invoice using a secret key (Ki) 410 and the signature is returned in message 630. Thereafter, processing proceeds to operation 760 where mobile station 20 awaits delivery of message 640. In the case where the product being delivered by seller 50 is a digital product, operation 760 would be executed. However, where the product being delivered is a tangible product, such as a basket of flowers, operation 760 may simply be the handing over that product to buyer 10 from seller 50. Thereafter, the buyer purchase module 1700 terminates execution in operation 770.

FIG. 8 is a flowchart of the seller sales module 1800, shown in FIG. 12, as utilized by an embodiment of the present invention. The seller sales module 1 800 is counterpart to the buyer purchase module 1700 and is utilized to check the validity of the digital certificate received from the buyer purchase module 1700.

Referring FIG. 8, the seller sales module 1800 includes operations 800 through operation 90 5. The seller sales module 800 begins execution in operation 800 and immediately proceeds to operation 810. In operation 810, the seller sales module 1800 waits for receipt of message 610 containing the certificate and service request. Upon receipt of m essage 610, processing proceeds to operation 820 where the validity of the certificate is verified and it is checked that any optional restrictions are not violated. Thereafter, in operation 830 the result of digital certificate verification is checked. This verification of the digital certificate is done online so that the seller 50 may determine whether the digital certificate provided by buyer 10 is still valid. The situation may arise where a certificate is issued by gateway 60 and later revoked when the subscriber reports a loss or theft of mobile station 20.

Still referring to FIG. 8, If the certificate is not valid then processing proceeds to operation 845 where the execution of the seller sales module 1 800 is terminated. However, if the certifi cate is valid, then processing proceeds to operation 840. In operation 840, it is determined whether the requested service complies with the optional restrictions applied. If the requested service does not comply with restrictions then again processing proceeds operation 845 where execution of the seller sales module 1800 terminates. However, if the restrictions are violated, then processing proceeds to operation 850. In operation 850, the invoice (I) is sent in message 620 to mobile station 20. In ope ration 860, the seller sales module 1800 waits for receipt of message 630. Upon receipt of message 630 containing signature (S), operation 870 checks the signature (S). Thereafter, in operation 880, a determination is made if signature (S) is valid. If the signature is not valid the processing again proceeds to operation 845 where the seller sales module 1800 is terminated. However, if the signature is valid, processing proceeds to operation 890 where the seller 50 creates an accounting record (AR) and stores it in the seller=s 50 local database. Thereafter, processing proceeds to operation 900 where the seller 50 proceeds to deliver the product or service desired. This may be done through the transmission of message 640 where the product is a digital product. Finally, the seller sales module 1800 terminates execution in operation 905.

FIGs. 9 through 11 illustrate the process whereby the seller 50 is able to receive payment for products and services sold using the embodiment of the present invention.

FIG. 9 is a diagram of the messages passed between the seller 50 and the gateway 60 in order to facilitate payment to the seller for services and goods provided to the buyer 10 in an example embodiment of the present invention. Only two messages are exch anged between seller 50 and gateway 60. Message

910 simply contains the current records accumulated by seller 50 within a finite period of time. However, as would be appreciated by one of ordinary skill in the art, each time an accounting record is gener ated it may be transmitted to gateway 60. Message 920 is a response supplied by gateway 60 to seller 50 indicating acceptance or rejection of the accounting records transmitted.

FIG. 10 is a flowchart of the seller billing module 1900, shown in FIG. 12, as utilized in an example embodiment of the present invention. The seller billing module 9000 includes operations 1000 through 1160 shown in FIG. 10. The seller billing module 9000 begins execution in operation 1000 and immediately proceeds to operation 1010. In operation 1010, variable i is set to 0. In operation 1020 a determination is made if any records remain that have not been incorporated into message 910. If no records are left then processing proceeds to operation 1030 where the seller billing module 1900 terminates execution. However, if no accounting records remain to be processed then processing proceeds to operation 1040 or they are placed in message 910. Thereafter, in operation 1050 i is incremented by 1. In operation 1060, a determination is made if any records remain to be processed. If records remain to be processed then processing proceeds operation 1070. In operation 1070, it is determined whether the variable i is less than the variable n which represents the maximum number of a ccounting records that may be put in message 910. If i is less than n then processing loops back to operation 1040 for further processing. However, if i is not less than n, then processing proceeds to operation 1080. In operation 1080 message 910 containing the accounting records is sent to seller 50. Thereafter, processing proceeds to operation 1090 where seller 50 awaits return of message 920 from gateway 60. Upon receipt of message 920 processing proceeds to operation 1110. In operation 1110, the r esponses from gateway 60 are accepted. In operation 1120, it is determined whether the response received indicates confirmation and thus an approval of the accounting record and payment thereof. If the responses are not confirmed in operation 1120, processing proceeds to operation 1130 where the accounting record is added to the error log. The error log would then be examined at some later point in time to determine the proper course of action. However, if the response equals a confirmation, then proces sing proceeds to operation 1140 where the accounting record is entered into a local internal log. Thereafter, in both the case of operation 1130 and 1140, processing proceeds to any unprocessed responses left in message 920. If there are any unprocessed responses, then processing loops back to operation 1110. However, if all responses have been processed, then processing proceeds to operation 1160 where execution of the seller billing module 1900 is terminated.

FIG. 11 is a flowchart of the gateway bill ing module 2000, shown in FIG. 12, as utilized in an example embodiment of the present invention. The gateway billing module 2000 is utilized to credit seller 50 with funds for purchases made by buyer 10 using mobile station 20. The gateway billing modul e 2000

17

also serves to verify the existence of a corresponding buyer=s record containing the digital certificate created by gateway certificate generation module 1600. Further, the gateway billing module 2000 also verifies the validity of the signature generated by the buyer purchase module 1700. As will be discussed in further detail ahead, using the verification of the digital certificate and the signature it is possible to insure that the buyer 10 is paying the correct amount for the purchase and that t he buyer 10 is only being billed once.

The gateway billing module 2000 includes operations 1200 through 1340 shown in FIG. 11 and begins execution in operation 1200. The gateway billing module 2000 upon startup in operation 1200 immediately proceeds to operation 1210. In operation 1210, the gateway billing module 2000 waits for the transmission and arrival of message 910 from the seller billing module 1900. In operation 1220, the message 910 is received from the seller 50 and processing proceeds to opera tion 1230. In operation 1230, an accounting record (AR) is extracted from message 910. Processing then proceeds to operation 1235 where it is determined whether this particular accounting record has previously been submitted. If the accounting record has previously been submitted then processing proceeds to operation 1300 were an error response is generated. However, if this particular accounting record has not been previously processed, then processing proceeds to operation 1240. In operation 1240, th e gateway 60 database is searched to find a corresponding record of the digital certificate for this sale. In operation 1250 a determination is made whether a record has been found. If no record is found then processing proceeds to operation 1300 where an error response for this particular accounting record is stored for transmission in message 920 to seller 50. However, if a corresponding record is discovered then processing proceeds to operation 1260.

Still referring to FIG. 11, the gateway billing module 2000, executing on gateway 60, proceeds to perform the second check to determine if the accounting record is correct. In operation 1260, the signature of buyer 10 is checked. Further, the associated restrictions for the digital certificate are che cked to determine if this accounting record violates any of these restrictions. In operation 1270, if either signature cannot be verified or if any restrictions are violated then processing proceeds to operation 1300 where an error response for this parti cular accounting record is stored for transmission in message 920. However, if the signature is verified and the restrictions are not violated then processing proceeds to operation 1280. In operation 1280, a call detailed record (CDR) is stored in the ga teway 60 database so that at some later time the seller 50 may be paid for all purchases by buyer=s 10 for that period of time. Further, the call detailed report is also charged to the buyer=s 10 account for that period of time. In GSM network this is do ne by sending the CDR from local operator to the home operator; the home operator then adds the transaction indicated in that CDR to buyer=s phone bill. Thereafter, in operation 1290, the response for this

18

accounting record is confirmed and stored as such for transmission in message 920 to the seller 50. Thereafter, processing proceeds from both operations 1290 and 1300 to operation 1310 where either a confirmed response or an error response is placed in the message 920. In operation 1320, it is determin ed if other accounting records remain in message 910 and need to be processed. If accounting records remain unprocessed in message 910 then processing loops back to operation 1230. However, if all accounting records have been processed then processing pr oceeds to operation 1330. In operation 1330, message 920 containing all responses to all the accounting records is transmitted to the seller 50 and processing for the gateway billing module terminates in operation 1340.

It should be noted that the seller billing module 1900 and the gateway billing module 2000 processed accounting records in a batch operation. However, as would be appreciated by one of ordinary skill in the art, an accounting record may also be transmitted from the seller 50 to the gateway 60 as they are generated in the seller sales module 1800. Such of an approach would increase the traffic between the seller 50 and gateway 60.

FIG. 12 is a modular configuration diagram of the embodiments of the present invention shown in FIGs. 5, 7, 8, 10, and 11. This modular configuration diagram illustrates the interconnection between modules in the present invention and the logical flow. It should be noted that the mobile station 20 certificate acquisition module 1500 is the only module that interfaces to the GSM authentication module 1400, the A3 algorithm module 430 and the A8 algorithm module 420, previously discussed in reference to FIG. 4. Using this embodiment of the present invention, the mobile station 20 need only be authenticated by the mobile telephone infrastructure for billing and authentication 90 upon startup and thus imposes a minimal burden upon the telecom mobile telephone infrastructure for billing and authentication 90.

Still referring to FIG. 12, once the mobile station 20 is authenticated the mobile station certificate acquisition module 1500 is able to obtain a digital certificate from the gateway 60 using the gateway certificate generation module 1600. With the certificate in the memory of mobile station 20 the buyer purchase module 1700 is able to make a purchase from a seller 50 in conjunction with the seller sales module 1800. The seller sales module 1800 generates an accounting record which the seller billing module 1900 is able to submit to the gateway 60. The gatewa y billing module 2000 in the gateway 60 will verify the accuracy of the accounting record and only charge the buyer 10 for the correct amount and only once for any purchase.

While we have shown and described only a few examples herein, it is understood th at numerous changes and modifications as known to those skilled in the art could be made to the present invention. For example, rather than a single digital certificate being transmitted in message 260, several could be transmitted at one time. In this m anner each certificate may have its own restrictions and when a buyer or

user 10 goes to make a purchase the certificate that most closely meets the requirements of the purchase may be transmitted to the seller 50. In addition, instead of transmitting mes sages containing M1, M2, and M3 as shown in FIG. 2 it is possible for all messages to be authenticated using a 32 -bit integrity key (Ki) that is part of the third generation standard security mechanism as specified in section 6.5 AAccess Link Data Integrity@ of 3G security document (3G TS 33.102 version 3.5.0 release 1999) which we incorporate herein by reference. Therefore, we do not wish to be limited to the details shown and described herein, but intend to cover all such changes and modifications as are encompassed by the scope of the appended claims.

CLAIMS

What is claimed is:

1.   A method of ordering, paying for and delivering goods and services using a mobile station, comprising:

accessing a gateway by the mobile station and transmitting an identification code for mobile station to the gateway;

verifying the identity of the mobile station by the gateway by accessing an authentication center and comparing variables computed by the mobile station and variables computed by the gateway;

delivering a digital certificate to the mobile station by the gateway when the identity of the mobile station have been verified; and

requesting a product or service from a seller and transmitting a digital signature, accompanied by the digital certificate for a signature verification key as payment to the seller.

2.   The method recited in claim 1, wherein the verifying the legitimacy of the gateway by the mobile station by comparing the variables computed by the gateway with the variables computed by the mobile station, further comprises:

transmitting from the mobile station to the gateway a session identification and an international mobile subscriber identifier;

transmitting the international mobile subscriber identifier from the gateway to the authentication center;

transmitting from the authentication center to the gateway a random number (RAND), a signed response (SRES), and an encryption key;

computing a variable M1 by the gateway and transmitting the variable M1 and the random number to the mobile station;

computing a variable M1' by the mobile station; and

verifying the legitimacy of the gateway when the variable M1 equals the variable M1'.

3.   The method recited in claim 2, wherein the integrity key (K) is computed by both the mobile station and the authentication center as a function of RAND and Ki, where RAND is a random number

21

issued by the authentication center, and Ki is a secret key contained within the authentication center and the mobile station.

4.   The method recited in claim 3, where RAND the in tegrity key (K) is transmitted by the of indications center to the gateway.

5.   The method recited in claim 1, further comprising:

computing a digital certificate by the gateway certifying the mobile station's public key (PK);

computing a variable M3 by the gateway and transmitting the variable M3 and the digital certificate to the mobile station;

computing a variable M3' by the mobile station;

verifying the legitimacy of the gateway when the variable M3 equals the variable M3'.

6.   The method recited in claim 5, wherein the variables M3 and M3' are computed using the formula $M3 = M3' = MAC(K, C)$, where MAC is a message authentication code function, K is an integrity key and C is the digital certificate created by the gateway to certify PK.

7.   The method recited in claim 1, wherein verifying the identity of the mobile station by the gateway accessing an authentication center and comparing variables computed by the mobile station and variables computed by the gateway, further comprises:

transmitting a signed response, a public key and a variable M2 computed by the mobile station to the gateway;

computing a variable M2' by the gateway;

comparing the variable M2 and the variable M2'; and

verifying the identity of the mobile station when variable M2 is equal to variable M2'.

8.   The method recited in claim 7, wherein variables M2 and M2' are computed using the formula $M2 = M2' = MAC(K, \{SRES\}, PK, [\{restrictions\}], [alias])$, wherein MAC is a message authentication code function, SRES is a signed response, K is an integrity key, PK is a public key, restrictions are limits on the certificate and alias is an alternate identification for the mobile station.

22

9.   The method recited in claim 1, wherein requesting a product or service from a seller and transmitting the digital signature, accompanied by the digital certificate for the signature verification key as payment to the seller, further comprises:

transmitting the certificate with the request for the product or service;

receiving an invoice from the seller indicating a price for the product or service;

computing a digital signature on the invoice;

·   approving the invoice by transmitting the digital signature to the seller; and

accepting delivery of the product or service by the buyer.

10.   The method recited in claim 9, wherein the seller upon transmission of the digital signature, further comprises:

verifying the digital signature;

verifying that restrictions associated with the digital certificate are not violated; and

creating the an accounting record for the product or service sold.

11.   The method recited in claim 10, further comprising:

transmitting from the seller to the gateway the accounting record having an invoice and digital signature of a customer of a home network operator service;

determining by the gateway that a corresponding record exists in a local database and the validity of the digital signature;

determining whether the invoice violates any restrictions contained in the corresponding record;

crediting the seller with an amount equal to that in the invoice; and

billing the buyer with the amount of the invoice.

12.   The method recited in claim 1, further comprising:

verifying the legitimacy of the gateway by the mobile station by comparing the variables comp uted by the gateway with the variables computed by the mobile station.

13.   The method recited in claim 11, wherein delivering a digital certificate to the mobile station by the gateway when the identity of the mobile station and the gateway have been verified, further comprises:

requesting a digital certificate by the mobile station from the gateway used to

order and pay for a product or service from a seller

14.   A system for ordering, paying for and delivering goods and services using a mobile station, comprising:

a GSM authentication module to verify that the mobile station is permitted to access a telecom infrastructure;

a mobile station certificate acquisition module to request a digital certificate for the mobile station from a gateway; and

a gateway certificate generation module to verify that the mobile station is authorized to receive the digital certificate by transmitting an international mobile subscriber identifier received from the mobile station to an authentication center, calculate variables based on information received from the authentication center and compare them to variables computed by the mobile station, and issue the digital certificate to the mobile station when the variables match.

15.   The system recited in claim 14, wherein the mobile station certificate acquisition module verifies that the gateway is authorized to issue the digital certificate through the use of comparing variables computed by the gateway and the mobile station.

16.   The system recited in claim 15, further c omprising:

a buyer purchase module to request the purchase of a good or service from a seller, present the digital certificate to the seller, receive an invoice and provide the seller with a digital signature approving the purchase of the good or service;

a seller sales module to verify the validity of the digital certificate and the validity of the digital signature, issue an invoice, generate an accounting record and deliver a product or service;

a seller billing module to transmit to the gateway the acc ounting record and receive a response indicating if the accounting record has been approved for payment; and

a gateway billing module to verify the accounting record and an accompanying signature, and issue a credit to the seller and debit to the buyer wh en the accounting record and the accompanying signature are verified.

17.   The system recited in claim 16, wherein the gateway certificate generation module transmits an international mobile subscriber identifier to the authentication center, receives a ra ndom

number, a signed response and an encryption key from the authentication center, computes a variable M1, M2', and M3 and verifies the validity of the mobile station by comparing variable M2 received from the mobile station with variable M2'.

18.   The system recited in claim 14, wherein the mobile station further comprises:

a subscriber identification module (SIM) used to compute a signed response and a ciphering key based on a secret key, installed by a home network operator service in the subscr iber identification module upon signing up for a service plan, and a random number obtained from an authentication center in the home network operator service;

an A3 algorithm module, contained in the SIM, is used to compute the signed response; and

an A8 algorithm module, contained in the SIM, is used to compute the ciphering key, wherein through the transmission of signed responses to and from the mobile station a telecommunication infrastructure is able to verify that the mobile station is authorized to access the telecommunication infrastructure and the gateway.

19.   A computer program embodied on a computer readable medium and executable by a computer for ordering, paying for and delivering goods and services using a mobile station, comprising:

a· GSM authentication code segment to verify that the mobile station is permitted to access a telecom infrastructure;

a mobile station certificate acquisition code segment to request a digital certificate for the mobile station from a gateway; and

a gateway certificate generation code segment to verify that the mobile station is authorized to receive the digital certificate by transmitting an international mobile subscriber identifier received from the mobile station to an authentication center, calculate variables based on information received from the authentication center and compare them to variables computed by the mobile station, and issue the digital certificate to the mobile station when the variables match.

20.   The system recited in claim 19, wherein the mo bile station certificate acquisition code segment verifies that the gateway is authorized to issue the digital certificate through the use of comparing variables computed by the gateway and the mobile station.

21.   The computer program recited in claim 19, further comprising:

a buyer purchase code segment to request the purchase of a good or service from a seller, present the digital certificate to the seller, receive an invoice and provide the seller with a digital signature approval the purchase of the good or service;
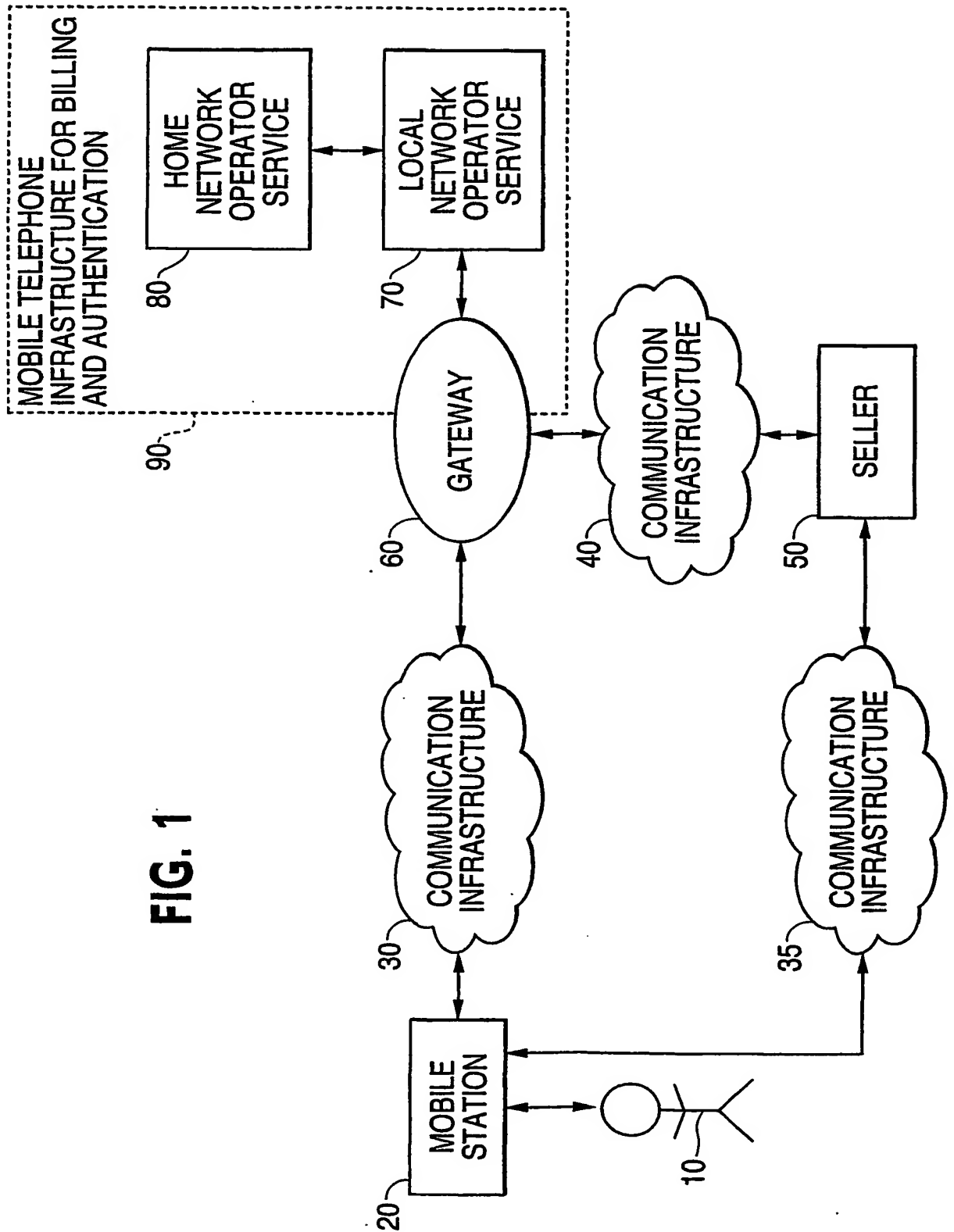
a seller sales code segment to verify the validity of the digital certificate and the validity of the digital signature, issue an invoice, generate an accounting record and deliver a product or service;

a seller billing code segment to transmit to the gateway the accounting record and receive a response indicating if the accounting record has been approved for payment; and

a gateway billing code segment to verify the accounting record and an accompanying signature, and issue a credit to the seller and debit to the buyer when the accounting record and the accompanying signature are verified.
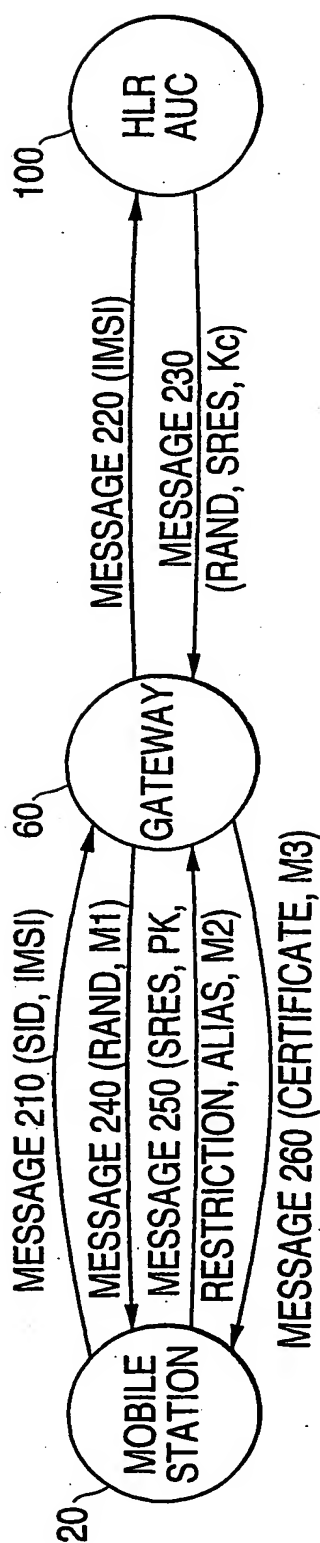
22.   The computer program recited in claim 20, wherein the mobile station certificate acquisition code segment transmits a session identification and an international mobile subscriber identifier to the gateway, receives a random number and a variable M1 from the gateway and verifies that the gateway is authentic by computing and comparing the variable M1' with M1.

23.   The computer program recited in claim 19, wherein the gateway certificate generation code segment transmits an international mobile subscriber identifier to the authentication center, receives a random number, a service response and an encryption key from the authentication center, computes a variable M1, M2', and M3 and verifies the validity of the mobile station by comparing variable M2 received from the mobile station with variable M2'.

FIG. 1

FIG. 2
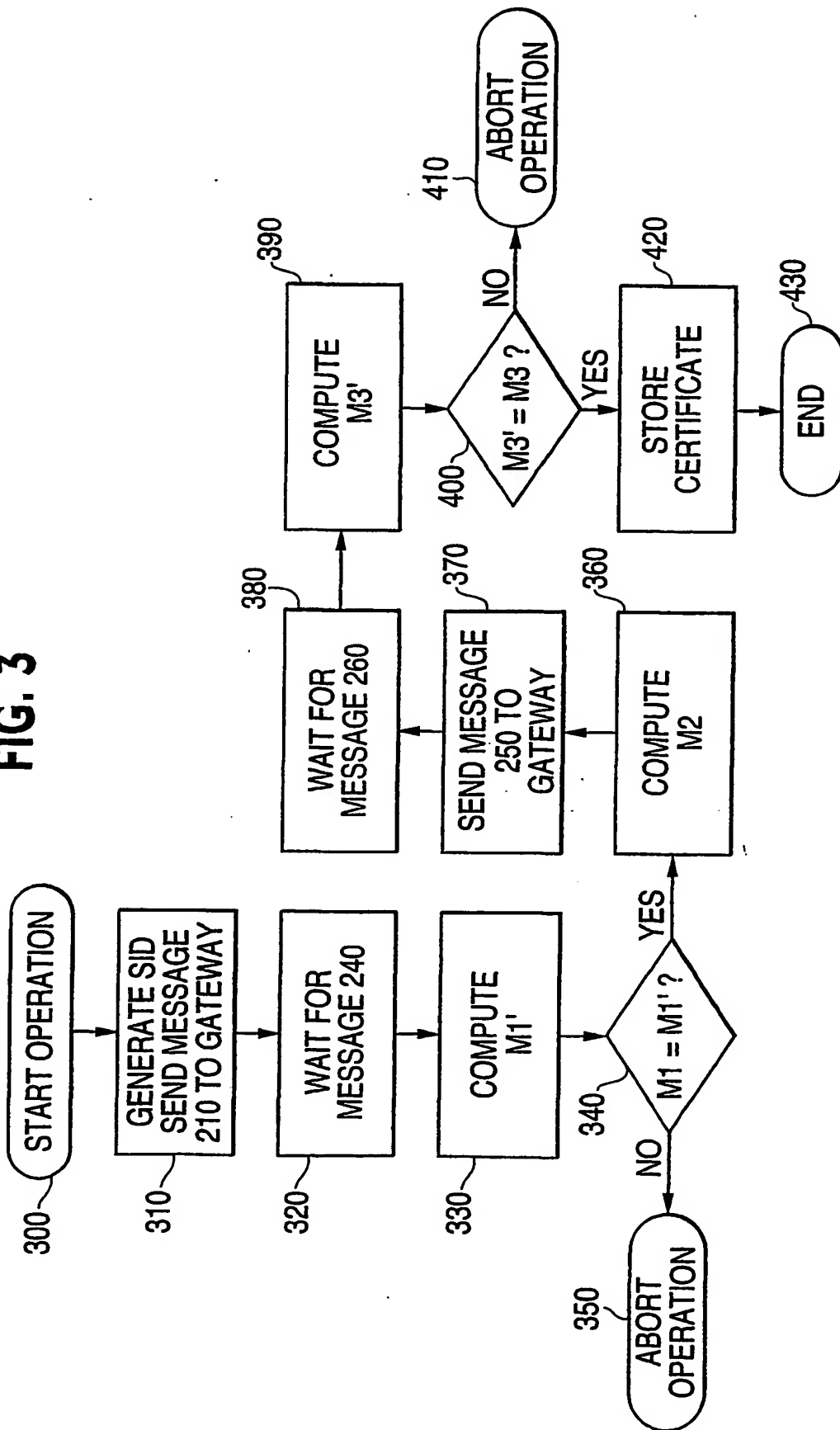
MOBILE STATION 20

GATEWAY 60

HLR AUC 100

MESSAGE 210 (SID, IMSI)

MESSAGE 240 (RAND, M1)

MESSAGE 250 (SRES, PK, RESTRICTION, ALIAS, M2)

MESSAGE 260 (CERTIFICATE, M3)

MESSAGE 220 (IMSI)

MESSAGE 230 (RAND, SRES, Kc)

FIG. 3

FIG. 4

FIG. 5

START OPERATION — 500

WAIT FOR MESSAGE 210 FROM MOBILE STATION — 510

SEND MESSAGE 220 TO HLR OVER MAP/D PROTOCOL — 520

WAIT FOR MESSAGE 230 — 530

COMPUTE M1 — 540

SEND MESSAGE 240 TO MOBILE STATION — 550

WAIT FOR MESSAGE 250 — 560

COMPUTE M2' — 570

M2' = M2 ? — 580

ABORT OPERATION — 590

NO

YES

COMPUTE M3 — 600

SEND MESSAGE 260 — 610

END — 270

FIG. 6

MESSAGE 610 (CERTIFICATE, REQUEST)

MESSAGE 620 (INVOICE)

MESSAGE 630 (SIGNATURE)

MESSAGE 640 (DELIVERY)

SELLER 50

MOBILE STATION 20

FIG. 7

```
        700 ─( START )
                 │
                 ▼
    710 ─┤ SEND MESSAGE 610 │
                 │
                 ▼
    720 ─┤ WAIT FOR MESSAGE 620 │
                 │
                 ▼
    730 ─┤ CHECK THE INVOICE (I) │
                 │
                 ▼
    740 ─< INVOICE (I) CORRECT? >─── NO ──▶ ( ABORT OPERATION ) ─ 750
                 │
                YES
                 │
                 ▼
    750 ─┤ S = SIGN (SK, I)
          SEND MESSAGE 630 │
                 │
                 ▼
    760 ─┤ WAIT FOR MESSAGE 640
          (SERVICE DELIVERY) │
                 │
                 ▼
        770 ─( END )
```

FIG. 8

FIG. 9

SELLER 50 — MESSAGE 910 (ACCOUNTING RECORD) → GATEWAY 60

GATEWAY 60 — MESSAGE 920 (RESPONSE) → SELLER 50

FIG. 10

1000 — (START)

1010 — [i = 0]

1020 — <RECORDS LEFT ?> — NO → (END OPERATION) — 1030

YES

1040 — [PUT RECORD IN MESSAGE 910]

1050 — [i = i + 1]

1070 YES — <i < n> ←YES— <RECORDS LEFT ?> — 1060

NO

1080 — [SEND MESSAGE 910]

1090 — [WAIT FOR MESSAGE 920]

1100 — [MESSAGE 920 RECEIVED]

YES ← <UNPROCESSED RESPONSE LEFT IN MESSAGE 920> — 1150

NO → (END OPERATION) — 1160

1110 — [TAKE RESPONSE FROM MESSAGE 920]

1140 — [ADD ENTRY TO INTERNAL LOG]

1120 — <RESPONSE = "CONFIRMED"> — YES

1130 — [ADD ENTRY TO LOG ERROR]

NO

FIG. 11

FIG. 12

GSM AUTHENTICATION MODULE ~1400

A8 ALGORITHM MODULE ~420

A3 ALGORITHM MODULE ~430

MOBILE STATION CERTIFICATE ACQUISITION MODULE ~1500

BUYER PURCHASE MODULE ~1700

SELLER SALES MODULE ~1800

GATEWAY CERTIFICATE GENERATION MODULE ~1600

GATEWAY BILLING MODULE ~2000

SELLER BILLING MODULE ~1900